REMARKS

Amendment of Claim 7

Consistent with the Examiner's suggestion in the June 13, 2005 Office Action, Applicant has hereby amended claim 7, by deleting the extra word "cryptogram."

Response to the §103 Rejections of Claims 1-23

In the June 13, 2005 Office Action, the Examiner rejected claims 1-23 under 35 U.S.C. §103(a) as alleged obvious over Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Wiley 1996 (hereinafter "Schneier") in view of U.S. Patent No. 6,718,467 issued to Trostle (hereinafter "Trostle"). Specifically, the Examiner asserts that the primary reference Schneier discloses *Diffie-Helman*'s key-exchange algorithm and *Schnorr*'s authentication protocol, which cover the claimed limitations of the present application.

Applicant respectfully disagrees, for the following reasons:

The independent claims 1 and 7-12 of the present application, from which claims 2-6 and 13-23 depend, expressly recite an authentication protocol that involves **five (5) cryptograms** A, B, X, C, Y, and Z. Specifically, A = F(g, *a*), B = F(g, *b*), X = F(A, *b*), C = F(A, *c*), Y = F(X, *c*), and Z = H(*a*, Y, *s*), while *g* is a pre-defined integer, *a*, *b*, and *c* are **three (3) random numbers** generated by the prover or the verifier computer, and *s* is the secret key. Note that the cryptogram Z includes the secret key *s*, and more importantly, *s* is "concealed" in Z by the presence of random number *a* and cryptogram Y.

Further, the authentication protocol recited by claims 1 and 7-12 includes **three (3) determinations** made by the prover and the verifier computer for verifying the correctness of the relation therebetween, which includes: a first determination made by the prover computer to see whether $X = F(B, a)$, a second determination made by the verifier computer to see whether $Y = F(C, b)$, and a third determination made by the verifier computer to see whether $A = J(v, Y, g, Z)$, in which v is the public key. Note that the third determination specifically verifies the relation between the public key v and the secret key s.

The primary reference Schneier cited by the Examiner in the June 16, 2005 Office Action fails to teach or suggest in any manner such an authentication protocol as recited by claims 1 and 7-12 of the present application.

Specifically, *Diffie-Helman*'s key-exchange algorithm as disclosed on page 513 of Schneier includes only two (2) cryptograms X and Y, while $X = g^x$ and $Y = g^y$, g is a prime integer that is not secret, and x, y are two (2) random integers generated by two participants Alice and Bob. Alice and Bob then respectively compute $k = Y^x$ and $k' = X^y$. Neither of the cryptograms X and Y includes a secret key s. Nor do the computations respectively carried out by Alice and Bob verify the relation between a public key v and a secret key s. Therefore, *Diffie-Helman*'s key-exchange algorithm disclosed by Schneier fails to provide any derivative basis for, and cannot be extrapolated to yield, the authentication protocol recited by claims 1 and 7-12 of the present application.

Schnorr's authentication protocol as disclosed on page 510 of Schneier teaches only two (2) cryptograms x and y, while $x = a^r$ and $y = (r + se)$, a is a pre-defined number, r and e are two (2) random numbers generated by Peggy (i.e., the prover) and Victor (i.e., the verifier), and s is the secret key. A single determination is then made by Victor (i.e., the verifier) to see whether $x = a^y v^e$, which functions to verify the correctness of the relation between Peggy (i.e., the prover) and Victor (i.e., the verifier). *Schnorr*'s authentication protocol disclosed by Schneier therefore also fails to provide any derivative basis for, and cannot be extrapolated to yield, the authentication protocol recited by claims 1 and 7-12 of the present application.

More importantly, nothing in the Schneier suggests modification of *Diffie-Helman*'s key-exchange algorithm and *Schnorr*'s authentication protocol.

Thus, the Schneier reference is deficient in teaching or suggesting the authentication protocol recited by claims 1 and 7-12 of the present application.

The secondary reference Trostle only discloses a password-based protocol established on an improved *Diffie-Helman*'s algorithm, and cannot remedy the deficiency of Schneier.

Based on the foregoing, claims 1 and 7-12 of the present application and their respective dependent claims 2-6 and 13-23 patentably distinguish over Schneier and Trostle, either taken singularly or in combination. Applicant respectfully requests the Examiner to reconsider, and upon reconsideration to withdraw, the rejections of Claims 1-23 of the present application.

Applicant further submits that this application is in condition for allowance, and a Notice of Allowance is respectfully requested. If any issues remain outstanding, incident to the formal allowance of the application, the Examiner is requested to contact the undersigned attorney at (516) 742-4343 to discuss same, in order that this application may be allowed and passed to issue at an early date.

Respectfully submitted,

Steven Fischman
Registration No. 34,594

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343
SF/MY:gc